IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA	:	
	:	CRIMINAL ACTION
v.	:	
	:	NO. 1:19-CR-515-JPB
CHARLES E. TAYLOR	:	

GOVERNMENT'S SENTENCING MEMORANDUM

The United States of America, by and through its counsel, Byung J. Pak, United States Attorney, and Nathan P. Kitchens, Assistant United States Attorney for the Northern District of Georgia, hereby submits this Sentencing Memorandum.

INTRODUCTION

The Government agrees that, by all accounts, the Defendant has made a positive impact on many in his life and has been dedicated to his family. The Government also agrees that the Defendant deserves credit for his early acceptance of responsibility and that he is not likely to commit other criminal conduct. And the Government ultimately agrees that a downward variance is proper in light of these considerations. Accordingly, the Government recommends a two-level downward variance below his sentencing guidelines range.

But the Defendant's request for a further significant downward variance to a non-custodial sentence is unwarranted and improper based on the 18 U.S.C. § 3553(a) factors. The Defendant conducted a multi-stage sabotage campaign against his former employer, BlueLinx Corporation ("BlueLinx"), using knowledge he gained during his employment to maximize losses to the company's IT infrastructure. The Defendant's conduct disrupted BlueLinx's communications, triggered a labor-intensive remediation process, and resulted in substantial business losses. Despite this damage, the Defendant requests a below-guidelines sentence of home confinement by attempting to minimize his culpability based on unsupported assertions, deflection, and victim-blaming. This request serves only to highlight his lack of remorse for his crime, which bolsters the need for a meaningful prison sentence.

The Defendant's conduct justifies a 24-month term of imprisonment, at the low end of the adjusted guidelines range with a two-level downward variance, in light of the grave seriousness of his offense and the need for general deterrence.

ARGUMENT

I. The Seriousness of the Offense Warrants a Meaningful Custodial Sentence.

The Defendant should receive a 24-month prison sentence because of the seriousness of his sabotage scheme, which was conducted with deliberation,

abused the sensitive information entrusted to him as a senior systems engineer, and caused profound losses to his victim. *See* 18 U.S.C. § 3553(a)(2)(A).

a. The deliberation and malicious intent required for Defendant's sabotage warrants a 24-month sentence.

More than a month after his resignation from BlueLinx, the Defendant hacked into the company without authorization and issued malicious commands that damaged its network. This was not a mistake, a poor decision in the heat of the moment, or an immature prank. By his own admission, this was outright sabotage planned over more than a month and designed to harass and harm his former employer. This sabotage scheme "required 'careful calculation and deliberation,'" which is an aggravating factor supporting a substantial sentence. *United States v. Matthews*, 477 F. App'x 585, 588 (11th Cir. 2012) (affirming upward variance of 19 months based, in part, on repeated deposits of stolen checks worth more than $400,000 over "prolonged period" of several months).

After BlueLinx acquired the Defendant's employer, Cedar Creek, in April 2018, the Defendant was disgruntled with the merger. PSR ¶ 8. Accordingly, the Defendant chose to resign on July 13, 2018. *Id.* ¶ 13. More than a month after his resignation, the Defendant struck against BlueLinx with a multi-stage attack. First, the Defendant "locked [BlueLinx] out of the routers" by connecting remotely with BlueLinx's network without authorization, using encryption techniques to mask his connection, and changing router passwords at company

warehouses. *Id.* ¶¶ 20, 22. The Defendant could not change all warehouse router passwords with a single command; instead, he had to connect remotely to individual warehouse routers to change each password. As a result, BlueLinx employees could not regain access to the routers, resulting in the replacement of more than forty routers. *Id.* ¶ 14. Second, the Defendant again connected remotely with BlueLinx's network without authorized access and issued a shutdown command for a critical communication server for BlueLinx's network, the Net001 server. *Id.* ¶¶ 9, 15. The server shutdown had a severe impact on BlueLinx's internal communications and business operations. *Id.* ¶ 15.

In sum, the Defendant deliberated for more than a month after his resignation from BlueLinx before issuing multiple malicious commands over several days to alter router passwords and shut down the Net001 server through his unauthorized access to the company's network. Each of these acts of sabotage was an independent criminal offense, which rebuts any suggestion that his criminal conduct was "aberrant behavior." *United States v. Orrega*, 363 F.3d 1093, 1097–98 (11th Cir. 2004) (noting that the USSG § 5K2.20 downward departure is reserved for "extraordinary" cases and holding that "commission of two criminal acts" by having two separate conversations with an undercover agent in enticement case "bars [defendant] from receiving an aberrant behavior departure").

The Defendant's sentencing memorandum underscores the extended planning and deliberation required to infiltrate BlueLinx's network and execute the sabotage scheme. According to the Defendant, his purported co-conspirator, Hunter Grubbs,[1] laid the groundwork for the sabotage "around the time of the Cedar Creek merger with BlueLinx" in April 2018 by reconfiguring network settings to stop the Net001 server data from automatically remounting in the event of a shutdown. (Doc. 13 at 5). Grubbs and the Defendant had multiple "discussions" about "go[ing] nuclear" by disabling BlueLinx's communications through a server shutdown. (*Id.*) By the Defendant's own account, the significant planning involved in executing the sabotage of BlueLinx bars the application of an aberrant behavior departure. *See Orrega*, 363 F.3d at 1098 (noting that defendant's conduct in two phone calls with undercover agent and driving to meeting place rebutted contention that crime was "committed without significant planning").

The Defendant's sentencing memorandum also highlights another factor justifying a meaningful prison sentence: his malicious intent in committing the offense. The Defendant suggests that he and his coworker Grubbs conspired to "go nuclear" by shutting down BlueLinx's network. (Doc. 13 at 5). Moreover, he

[1] Although the sentencing memorandum repeatedly refers to Grubbs as the "mastermind" of the scheme, it points to no evidence of Grubbs's planning of or participation in sabotage prior to the network shutdown.

explains his targeting of BlueLinx by comparing the company's merger to "the Huns invading Rome." (*Id.* at 13). Based on the Defendant's account, he knowingly transmitted commands to intentionally cause damage to BlueLinx's network, conduct akin to a violation of 18 U.S.C. § 1030(a)(5)(A). The United States Sentencing Commission recognized that such offenses committed with malicious intent were "singled out by Congress as being of particular concern" and created a four-level sentencing enhancement under USSG § 2B1.1(b)(19)(A)(ii) to deter such conduct. *Report to Congress: Increased Penalties for Cyber Security Offenses*, U.S. Sentencing Commission, at 9 (May 2003), *available at* https://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/computer crime/200304_RtC_Increased_ Penalties_Cyber_Security.pdf. Because the Defendant was instead convicted of an offense under § 1030(a)(5)(B), this four-level enhancement does not apply here. But given the Defendant's admission that he intended to cause damage to the network consistent with a violation of Section 1030(a)(5)(A), the guidelines range here, if anything, understates his culpability by not accounting for his malicious intent in committing this offense.

Based on the Defendant's multiple criminal acts of sabotage planned with deliberation and a malicious intent to harm the victim, the seriousness of his offense justifies a meaningful sentence of imprisonment.

b. The Defendant's abuse of trust warrants a 24-month sentence.

The Defendant's sabotage was particularly destructive because he took advantage of his employer's trust to cripple the computer network he had been paid to safeguard for more than five years. Specifically, the Defendant joined Cedar Creek as a systems administrator in January 2013 and was subsequently promoted in 2015 to senior systems engineer. PSR ¶ 12. After BlueLinx's acquisition of Cedar Creek, the Defendant maintained the same role until his resignation in July 2018. *Id.* ¶¶ 12–13. As a network systems engineer, the Defendant was entrusted to secure the company's network and protect it from threats, and he acquired specific knowledge of the network's functioning and vulnerabilities. But instead of protecting his employer, he betrayed it. In executing his scheme, the Defendant used his specialized knowledge to infiltrate the network remotely and to identify which server to shut down to maximize the destructive impact. *Id.* ¶ 38. The Defendant thus properly received a two-level adjustment pursuant to USSG § 3B1.3 for his use of special skills based on his IT training and education. *Id.* But the Defendant's misconduct also abused the trust of his employer, which serves as an independent basis for this enhancement.

Based on the depth of the Defendant's relationship with his victim and his misuse of the specialized knowledge entrusted to him, his betrayal of the victim's trust reflects a calculating spirit supporting more severe punishment.

c. The gravity of losses suffered by the victim warrants a 24-month sentence.

The toll suffered by BlueLinx reflects the severity of the Defendant's crime. While the loss amount exceeding $800,000 is substantial, it does not capture the full impact of the Defendant's sabotage. The true reflection of harm to the company is found not in the raw numbers but in the strain created for hundreds of employees trying to do their jobs with normal internal communications derailed and the painstaking remediation and investigation required in the following weeks to ensure that the company's network was not still at risk. The Government hopes to highlight the victim's story at the sentencing hearing.

In an effort to minimize the seriousness of his offense, the Defendant's sentencing memorandum acknowledges his agreement to a loss amount exceeding $550,000 while nonetheless questioning every category of loss. (Doc. 13 at 3). As the probation officer notes, this argument is curious when the Defendant has agreed to pay roughly $834,000 as restitution to BlueLinx for its losses, which corresponds with each and every category of loss detailed in the loss amount calculation. PSR ¶ 31. Despite this agreement, the Defendant presents three flawed arguments that reveal a discouraging lack of remorse for the extent of damage caused by his sabotage.

The Defendant's discussion of the loss categories hinges on unsupported assertions and assumptions contradicted by evidence provided by BlueLinx. For

example, the Defendant claims, without any citation or evidentiary support, that BlueLinx could have replaced the equivalent routers he rendered inaccessible for a cost of $10,000 and that BlueLinx was "in the process of changing the routers before the shutdown." (Doc. 13 at 7). But invoices provided by BlueLinx (and produced to the Defendant) established that the company purchased the routers in the days and weeks following his sabotage, not before the shutdown. The Defendant also baldly asserts that the IT remediation cost calculated by BlueLinx "seems excessive" based on his old hourly wage, (*id.* at 8), but he provides no competing estimate to counter BlueLinx's data.

Most glaringly, the Defendant asserts, without evidence, that the business interruption cost overstates the loss because "the supposed sales [lost] during the days the computers were down were deferred to subsequent days." (*Id.*) This assumption both ignores data provided by BlueLinx and misrepresents the nature of its customers. Contrary to the Defendant's assumption, BlueLinx's sales data, which was shared with the Defendant, did not show a surge in sales in the days following the sabotage that compensated for the sales decline coinciding with the Net001 server shutdown. Moreover, as noted in the PSR, the $353,826 in business interruption losses was based on a decline of "gross margin" over two days, not gross revenue. PSR ¶ 31. The loss amount under Section 2B1.1 of the Sentencing Guidelines includes "any revenue lost" from the computer fraud

offense. USSG § 2B1.1, cmt. n.3(A)(v)(III). The gross margin decline over the two-day period corresponding with the shutdown was a fraction of the revenue decline over that same period; if anything, the business interruption cost calculated for the Defendant's offense thus significantly understates the loss amount applicable under Section 2B1.1. The Government nevertheless submits that the substantially lower "gross margin" calculation is a reasonable estimate of the loss if the Defendant's deferred sales argument is credited.

Aside from offering baseless speculation, the Defendant attempts to deflect blame from his own culpability by claiming that his former co-worker, Grubbs, caused much of the losses. Specifically, the Defendant asserts that if Grubbs had provided helpful information to BlueLinx after the Defendant shut down the Net001 server, "there would have been no need for a forensic investigation team, and there would have been no revenue losses at all." (Doc. 13 at 11). But by the Defendant's own account, he and Grubbs conspired to damage BlueLinx's business through a shutdown of the Net001 server as part of their plan to "go nuclear." (*Id.* at 5). Accordingly, if the Defendant's story about the "nuclear" plan is true, Grubbs's acts subsequent to the server shutdown were in furtherance of their jointly undertaken criminal plan to damage BlueLinx, which would be relevant conduct attributable to the Defendant. USSG § 1B1.3(a)(1)(B). The Defendant thus was properly held accountable for the business interruption costs

and remediation expenses he claims were triggered by Grubbs's inaction and misdirection.

Finally, and most troublingly, the Defendant resorts to victim-blaming by suggesting that BlueLinx should have done more to mitigate its own losses. Specifically, he insults BlueLinx's IT personnel by claiming that "[a] competent IT person could have gotten the business operation up and running in hours" in the wake of the server shutdown. (Doc. 13 at 9). He casts more blame on BlueLinx employees for their inability to access warehouse routers after his password changes by suggesting they "did not know how to or were unwilling to access the routers by simply resetting the passwords." (*Id.*). And the Defendant analogizes BlueLinx's acquisition of his former employer to "the Huns invading Rome," with the caveat that comparing the victim to barbarian hordes does not "condone the [Defendant's] conduct." (Doc. 13 at 13). The Defendant's apparent animus for the victim calls into question his acceptance of his own culpability and remorse for his criminal acts of sabotage, which itself justifies a more severe sentence.

In short, the record reflects that the Defendant executed his sabotage scheme with deliberation and malicious intent over a considerable period of time, abused the victim's trust in using the specialized knowledge acquired in his job against the company, and caused serious harm to the victim company. The

seriousness of the offense requires a prison sentence within the adjusted guidelines range.

II. The Need for General Deterrence Warrants a Substantial Custodial Sentence.

A meaningful prison sentence is also necessary based on the need for general deterrence against further criminal conduct. *See* 18 U.S.C. § 3553(a)(2)(B).

Although the Government agrees that there is a low risk the Defendant will re-offend, the devastating scale of his sabotage supports a sentence that recognizes an "important goal of sentencing in a white-collar crime prosecution: the need for general deterrence." *United States v. Kuhlman*, 711 F.3d 1321, 1328 (11th Cir. 2013). The Eleventh Circuit has recognized that "[b]ecause economic and fraud-based crimes are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence." *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (internal quotation marks and alteration omitted). The Eleventh Circuit in *Kuhlman* "encourage[d] our district court colleagues to keep in mind that . . . '[c]riminals who have the education and training that enables people to make a decent living without resorting to crime are more rather than less culpable than their desperately poor and deprived brethren in crime.'" 711 F.3d at 1329 (quoting *United States v. Stefonek*, 179 F.3d 1030, 1038 (7th Cir. 1999)); *see also United States v. Hayes*, 762 F.3d 1300, 1311 (11th Cir. 2014) (reversing downward variance to

probation from guidelines range of 41–51 months when "the sentences do not provide for general deterrence because [t]he threat of spending time on probation simply does not, and cannot, provide the same level of deterrence as can the threat of incarceration in a federal penitentiary for a meaningful period of time" (quotation marks omitted, alteration in original)).

The damaging sabotage here shows the importance of deterrence given the magnitude of the losses suffered. The Defendant was a highly experienced and well-trained IT professional at the time he sabotaged BlueLinx because he was disgruntled with a corporate merger. PSR ¶¶ 12, 84–86. An employee hacking into his former employer's computer system to damage the network is a "serious and complex" offense supporting the need for a substantial prison sentence. *United States v. Eubanks*, 753 F. App'x 806, 816 (11th Cir. 2018) (affirming 84-month sentence as substantively reasonable given seriousness of offense when defendant hacked into former employer, accessed personal information of employees, destroyed files, and obtained credit card numbers to make unauthorized purchases). Indeed, the FBI has warned the private sector about the "significant losses" caused by cyber insider threat actors, many of whom are also "disgruntled employees" who "most often are motivated by revenge." *Cyber Threat Actors Disrupt Networks and Steal Data, Inflicting Significant Losses to US Businesses*, FBI-Cyber Division (Apr. 23, 2019), *available at*

https://www.sc.edu/study/colleges_schools/law/centers/cybersecurity/_docs/fbi_cyber_pin/2019/fbi_pin-20190423-001.pdf. Given the disruption caused by the Defendant with malicious intent against his former employer, a non-custodial sentence would convey the message "that would-be white-collar criminals stand to lose . . . practically none of their liberty" for committing similarly damaging offenses. *Martin*, 455 F.3d at 1240. The sentence imposed instead should send a strong message that IT professionals cannot abuse the trust placed in them to damage the networks they are entrusted to protect and that malicious sabotage will be severely punished.

III. The Defendant's Request for Probation Is Substantively Unreasonable under the 18 U.S.C. §3553(a) Factors.

Despite these significant aggravating factors, the Government agrees with the Defendant that there are mitigating circumstances that support a downward variance from his guidelines range of 30–37 months. When FBI agents confronted the Defendant with the undercover recordings made by Grubbs, the Defendant admitted his culpability in the initial meeting. This admission is a positive sign that he recognizes his wrongdoing, which lessens the need for deterrence under Section 3553(a). Furthermore, although the Sentencing Guidelines include losses for computer fraud offenses "regardless of whether such pecuniary harm was reasonably foreseeable," USSG § 2B1.1, cmt. n.3(A)(v)(III), his sabotage triggered remediation costs beyond what he likely anticipated when he committed his

crime. And the history and characteristics of the Defendant, as reflected in the character letters submitted with his sentencing memorandum, suggest that the Defendant has done laudable acts and is unlikely to re-offend. For all of these reasons, the Government believes that a two-level downward variance, and a sentence at the low-end of the adjusted guidelines range, is proper based on its consideration of the Section 3553(a) factors.

But the Defendant's request for an even further downward variance to probation with a condition of home detention goes too far. This request, which amounts to at least an 8-level downward variance,[2] is not justified by the record or by the COVID-19 pandemic and would be substantively unreasonable under the Section 3553(a) factors.

The Defendant frames his request for home detention as a downward departure for age and physical condition under USSG §§ 5H1.1 & 5H1.4, but the plain language of those provisions reveals their unsuitability here. Both downward departures note that age and physical condition are not ordinarily relevant guidelines considerations unless the Defendant's advanced age or physical impairment is "present to an unusual degree." USSG §§ 5H1.1 & 5H1.4.

[2] Pursuant to the United States Sentencing Guidelines, a sentence of probation with a condition of home detention conforms with the guidelines only if the applicable guideline range is in Zone B of the Sentencing Table. USSG § 5C1.1(c)(3). The top of Zone B is Offense Level 11 with Criminal History Category I; the Defendant's current Offense Level is 19. (PSR ¶ 43).

A Section 5H1.1 departure may be proper when the defendant is "elderly and infirm," and a Section 5H1.4 departure requires evidence of an "extraordinary physical impairment," such as a case involving a "seriously infirm defendant." *Id.* Here, the Defendant turned 60 last month, and the Defendant does not argue that this renders him "elderly and infirm," nor does he identify any health conditions that constitute "extraordinary physical impairment." *See United States v. Stumpner*, 174 F. App'x 522, 525 (11th Cir. 2006) (affirming denial of Section 5H1.1 departure and reasonableness of 292-month sentence for 74-year-old defendant); *United States v. Paradies*, 14 F. Supp. 2d 1315, 1320 (N.D. Ga. 1998) (denying Section 5H1.1 and 5H1.4 departures for 76-year-old defendant with osteoarthritis and chest pains). In short, the Defendant identifies no age or health circumstances unique to him that would justify a downward departure pursuant to Sections 5H1.1 or 5H1.4.

Instead, the Defendant essentially proposes blanket immunity from incarceration for non-violent felons because of the COVID-19 pandemic, which he suggests presents "extraordinary and compelling reasons to reduce his sentence." (Doc. 13 at 16–19). The Defendant acknowledges that "he does not suffer from any additional underlying health conditions that render him especially vulnerable to COVID-19" and points to no criteria under CDC guidelines that would qualify him as being at higher risk for severe illness from

COVID-19.[3] (Doc. 13 at 17). The COVID-19 pandemic thus does not establish that he is "elderly" or suffers "extraordinary physical impairment" to justify a downward departure, nor is a worldwide pandemic a proper consideration under the Section 3553(a) factors.

The Government does not minimize the risks that COVID-19 poses in the federal prison system and society at large. Indeed, the Bureau of Prisons has undertaken "extensive and professional efforts to curtail the virus's spread," *United States v. Raia*, 954 F.3d 594, 597 (3d Cir. 2020), including regularly updating its COVID-19 modified operating procedures that require enhanced screening of prisoners, issuing masks for daily wear, prohibiting social visitors, and quarantining of new inmates prior to placement in a BOP facility. BOP COVID-19 Modified Operations Plan, https://www.bop.gov/coronavirus/covid19_status.jsp. In addition, as noted by the Defendant, the Attorney General expanded BOP's authority to review inmates for COVID-19 risk factors and, where appropriate, designate them for home confinement, which has resulted in the placement of more than 3,000 inmates on home confinement since March 26, 2020. *See* COVID-19 Home

[3] The Defendant claims that he is at "high risk" and especially vulnerable to COVID-19 because he turned 60 last month, but CDC guidelines state that people 65 and older are in the high-risk category. *See* People Who Are At Higher Risk, Centers for Disease Control & Prevention, *available at* https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/people-at-higher-risk.html.

Confinement Information, https://www.bop.gov/coronavirus/index.jsp. The BOP has extensive experience in making these assessments, and the Defendant does not suggest that BOP would fail to follow these guidelines in assessing his placement and safeguarding his health in light of the pandemic. The mere existence of the COVID-19 pandemic, which poses a general threat to every non-immune person in the country, thus does not alone provide "extraordinary and compelling reasons" for a substantial departure or variance to home detention.[4]

Nor would a non-custodial sentence be proper under the Section 3553(a) factors. A line of cases in the Eleventh Circuit have vacated fraud sentences with minimal or no terms of incarceration as substantively unreasonable. *See, e.g.*, *Kuhlman*, 711 F.3d 1321, 1328–29; *Martin*, 455 F.3d at 1230, 1238–39; *United States v. Crisp*, 454 F.3d 1285, 1291 (11th Cir. 2006) (vacating sentence of 5 hours' imprisonment for $480,000 bank fraud case after defendant provided substantial assistance because punishment did "not reflect the seriousness of the crime, promote respect for the law, and provide just punishment for the offense . . ., nor [did] it afford adequate deterrence to criminal conduct."). In *Hayes*, the district court sentenced a 67-year-old business owner to probation, with 6–12 months of

[4] The Sentencing Guidelines define "extraordinary and compelling reasons" supporting a reduction of a previously imposed sentence under 18 U.S.C. § 3582(c) to include four criteria, none of which is satisfied by the Defendant. *See* U.S.S.G. § 1B1.13 cmt. n.1.

home confinement, after varying downward from a guidelines range of 41–51 months based on his $600,000 bribery scheme. 762 F.3d at 1306. Although the district court found that the defendant provided substantial assistance to the government, "was genuinely remorseful, was not likely to commit further crimes, and was not a risk to the public," *id.* at 1308, the Eleventh Circuit vacated the sentence as substantively unreasonable given the seriousness of the offense and the failure to provide for general deterrence. *Id.* at 1310–11. The same Section 3553(a) factors support a 24-month sentence at the low end of the adjusted guidelines range given the more than $800,000 loss here.

CONCLUSION

Based on a full consideration of the Section 3553(a) factors, the Government recommends a low-end guidelines sentence after a two-level downward variance is applied for the Defendant's early acceptance of responsibility and the history and characteristics of the Defendant. A substantial prison sentence is required based on the seriousness of the Defendant's sabotage, his betrayal of an employer who entrusted him with safeguarding its network, and the need to deter other disgruntled employees from engaging in similar schemes to damage their employers. Such a sentence not only provides a fair result in light of the history and characteristics of the Defendant, but also

adequately reflects the gravity of his harm and sends a strong message that sabotage and computer fraud from company insiders will not be tolerated.

Respectfully submitted,

Byung J. Pak
UNITED STATES ATTORNEY

/s Nathan P. Kitchens
NATHAN P. KITCHENS
ASSISTANT U.S. ATTORNEY
600 Richard B. Russell Building
75 Ted Turner Dr., SW
Atlanta, Georgia 30303
Phone: (404) 581-6185
Fax: (404) 581-6181
Email: nathan.kitchens@usdoj.gov
Ga. Bar No. 263930

CERTIFICATE OF SERVICE

I hereby certify that the above was prepared using Book Antiqua 13-point font, and that I have caused a copy of the foregoing to be served upon Counsel for the Defendant by electronic filing:

This 23rd day of May 2020.

/s Nathan P. Kitchens
NATHAN P. KITCHENS